

113TH CONGRESS  
1ST SESSION

# H. R. 1163

To amend chapter 35 of title 44, United States Code, to revise requirements relating to Federal information security, and for other purposes.

---

## IN THE HOUSE OF REPRESENTATIVES

MARCH 14, 2013

Mr. ISSA (for himself, Mr. CUMMINGS, Mr. MICA, and Mr. CONNOLLY) introduced the following bill; which was referred to the Committee on Oversight and Government Reform

---

## A BILL

To amend chapter 35 of title 44, United States Code, to revise requirements relating to Federal information security, and for other purposes.

1       *Be it enacted by the Senate and House of Representa-  
2 tives of the United States of America in Congress assembled,*

**3 SECTION 1. SHORT TITLE.**

4       This Act may be cited as the “Federal Information  
5 Security Amendments Act of 2013”.

1 SEC. 2. COORDINATION OF FEDERAL INFORMATION POL-

2 ICY.

3 Chapter 35 of title 44, United States Code, is amend-  
4 ed by striking subchapters II and III and inserting the  
5 following:

6 “SUBCHAPTER II—INFORMATION SECURITY

7 **“§ 3551. Purposes**

8 “The purposes of this subchapter are to—

9       “(1) provide a comprehensive framework for en-  
10 suring the effectiveness of information security con-  
11 trols over information resources that support Fed-  
12 eral operations and assets;

13       “(2) recognize the highly networked nature of  
14 the current Federal computing environment and pro-  
15 vide effective Governmentwide management and  
16 oversight of the related information security risks,  
17 including coordination of information security efforts  
18 throughout the civilian, national security, and law  
19 enforcement communities assets;

20       “(3) provide for development and maintenance  
21 of minimum controls required to protect Federal in-  
22 formation and information systems;

23       “(4) provide a mechanism for improved over-  
24 sight of Federal agency information security pro-  
25 grams and systems through a focus on automated

1 and continuous monitoring of agency information  
2 systems and regular threat assessments;

3 “(5) acknowledge that commercially developed  
4 information security products offer advanced, dy-  
5 namic, robust, and effective information security so-  
6 lutions, reflecting market solutions for the protection  
7 of critical information systems important to the na-  
8 tional defense and economic security of the Nation  
9 that are designed, built, and operated by the private  
10 sector; and

11 “(6) recognize that the selection of specific  
12 technical hardware and software information secu-  
13 rity solutions should be left to individual agencies  
14 from among commercially developed products.

15 **“§ 3552. Definitions”**

16 “(a) SECTION 3502 DEFINITIONS.—Except as pro-  
17 vided under subsection (b), the definitions under section  
18 3502 shall apply to this subchapter.

19 “(b) ADDITIONAL DEFINITIONS.—In this subchapter:  
20 “(1) ADEQUATE SECURITY.—The term ‘ade-  
21 quate security’ means security commensurate with  
22 the risk and magnitude of the harm resulting from  
23 the unauthorized access to or loss, misuse, destruc-  
24 tion, or modification of information.

1           “(2) AUTOMATED AND CONTINUOUS MONI-  
2       TORING.—The term ‘automated and continuous  
3       monitoring’ means monitoring, with minimal human  
4       involvement, through an uninterrupted, ongoing real  
5       time, or near real-time process used to determine if  
6       the complete set of planned, required, and deployed  
7       security controls within an information system con-  
8       tinue to be effective over time with rapidly changing  
9       information technology and threat development.

10          “(3) INCIDENT.—The term ‘incident’ means an  
11       occurrence that actually or potentially jeopardizes  
12       the confidentiality, integrity, or availability of an in-  
13       formation system, or the information the system  
14       processes, stores, or transmits or that constitutes a  
15       violation or imminent threat of violation of security  
16       policies, security procedures, or acceptable use poli-  
17       cies.

18          “(4) INFORMATION SECURITY.—The term ‘in-  
19       formation security’ means protecting information  
20       and information systems from unauthorized access,  
21       use, disclosure, disruption, modification, or destruc-  
22       tion in order to provide—

23           “(A) integrity, which means guarding  
24       against improper information modification or

1 destruction, and includes ensuring information  
2 nonrepudiation and authenticity;

3 “(B) confidentiality, which means pre-  
4 serving authorized restrictions on access and  
5 disclosure, including means for protecting per-  
6 sonal privacy and proprietary information; and

7 “(C) availability, which means ensuring  
8 timely and reliable access to and use of infor-  
9 mation.

10 “(5) INFORMATION SYSTEM.—The term ‘infor-  
11 mation system’ means a discrete set of information  
12 resources organized for the collection, processing,  
13 maintenance, use, sharing, dissemination, or disposi-  
14 tion of information and includes—

15 “(A) computers and computer networks;

16 “(B) ancillary equipment;

17 “(C) software, firmware, and related proce-  
18 dures;

19 “(D) services, including support services;  
20 and

21 “(E) related resources.

22 “(6) INFORMATION TECHNOLOGY.—The term  
23 ‘information technology’ has the meaning given that  
24 term in section 11101 of title 40.

25 “(7) NATIONAL SECURITY SYSTEM.—

1                 “(A) DEFINITION.—The term ‘national se-  
2         curity system’ means any information system  
3         (including any telecommunications system) used  
4         or operated by an agency or by a contractor of  
5         an agency, or other organization on behalf of an  
6         agency—

7                 “(i) the function, operation, or use of  
8         which—

9                 “(I) involves intelligence activi-  
10         ties;

11                 “(II) involves cryptologic activi-  
12         ties related to national security;

13                 “(III) involves command and  
14         control of military forces;

15                 “(IV) involves equipment that is  
16         an integral part of a weapon or weap-  
17         ons system; or

18                 “(V) subject to subparagraph  
19         (B), is critical to the direct fulfillment  
20         of military or intelligence missions; or

21                 “(ii) is protected at all times by proce-  
22         dures established for information that have  
23         been specifically authorized under criteria  
24         established by an Executive order or an  
25         Act of Congress to be kept classified in the

1 interest of national defense or foreign pol-  
2 icy.

3                         “(B)                     EXCEPTION.—Subparagraph  
4                         (A)(i)(V) does not include a system that is to  
5                         be used for routine administrative and business  
6                         applications (including payroll, finance, logis-  
7                         tics, and personnel management applications).

8               “(8) THREAT ASSESSMENT.—The term ‘threat  
9               assessment’ means the formal description and eval-  
10          uation of threat to an information system.

## **11 “§ 3553. Authority and functions of the Director**

12        "(a) IN GENERAL.—The Director shall oversee agen-  
13 cy information security policies and practices, including—

14               “(1) developing and overseeing the implementa-  
15               tion of policies, principles, standards, and guidelines  
16               on information security, including through ensuring  
17               timely agency adoption of and compliance with  
18               standards promulgated under section 11331 of title  
19               40;

20               “(2) requiring agencies, consistent with the  
21 standards promulgated under such section 11331  
22 and the requirements of this subchapter, to identify  
23 and provide information security protections com-  
24 mensurate with the risk and magnitude of the harm

1       resulting from the unauthorized access, use, disclosure,  
2       disruption, modification, or destruction of—  
3               “(A) information collected or maintained  
4               by or on behalf of an agency; or  
5               “(B) information systems used or operated  
6               by an agency or by a contractor of an agency  
7               or other organization on behalf of an agency;  
8               “(3) coordinating the development of standards  
9       and guidelines under section 20 of the National In-  
10      stitute of Standards and Technology Act (15 U.S.C.  
11      278g-3) with agencies and offices operating or exer-  
12      cising control of national security systems (including  
13      the National Security Agency) to assure, to the max-  
14      imum extent feasible, that such standards and  
15      guidelines are complementary with standards and  
16      guidelines developed for national security systems;  
17               “(4) overseeing agency compliance with the re-  
18      quirements of this subchapter, including through  
19      any authorized action under section 11303 of title  
20      40, to enforce accountability for compliance with  
21      such requirements;  
22               “(5) reviewing at least annually, and approving  
23      or disapproving, agency information security pro-  
24      grams required under section 3554(b);

1               “(6) coordinating information security policies  
2 and procedures with related information resources  
3 management policies and procedures;

4               “(7) overseeing the operation of the Federal in-  
5 formation security incident center required under  
6 section 3555; and

7               “(8) reporting to Congress no later than March  
8 1 of each year on agency compliance with the re-  
9 quirements of this subchapter, including—

10               “(A) an assessment of the development,  
11 promulgation, and adoption of, and compliance  
12 with, standards developed under section 20 of  
13 the National Institute of Standards and Tech-  
14 nology Act (15 U.S.C. 278g–3) and promul-  
15 gated under section 11331 of title 40;

16               “(B) significant deficiencies in agency in-  
17 formation security practices;

18               “(C) planned remedial action to address  
19 such deficiencies; and

20               “(D) a summary of, and the views of the  
21 Director on, the report prepared by the Na-  
22 tional Institute of Standards and Technology  
23 under section 20(d)(10) of the National Insti-  
24 tute of Standards and Technology Act (15  
25 U.S.C. 278g–3).

1        “(b) NATIONAL SECURITY SYSTEMS.—Except for the  
2 authorities described in paragraphs (4) and (8) of sub-  
3 section (a), the authorities of the Director under this sec-  
4 tion shall not apply to national security systems.

5        “(c) DEPARTMENT OF DEFENSE AND CENTRAL IN-  
6 TELLIGENCE AGENCY SYSTEMS.—(1) The authorities of  
7 the Director described in paragraphs (1) and (2) of sub-  
8 section (a) shall be delegated to the Secretary of Defense  
9 in the case of systems described in paragraph (2) and to  
10 the Director of Central Intelligence in the case of systems  
11 described in paragraph (3).

12       “(2) The systems described in this paragraph are sys-  
13 tems that are operated by the Department of Defense, a  
14 contractor of the Department of Defense, or another enti-  
15 ty on behalf of the Department of Defense that processes  
16 any information the unauthorized access, use, disclosure,  
17 disruption, modification, or destruction of which would  
18 have a debilitating impact on the mission of the Depart-  
19 ment of Defense.

20       “(3) The systems described in this paragraph are sys-  
21 tems that are operated by the Central Intelligence Agency,  
22 a contractor of the Central Intelligence Agency, or another  
23 entity on behalf of the Central Intelligence Agency that  
24 processes any information the unauthorized access, use,  
25 disclosure, disruption, modification, or destruction of

1 which would have a debilitating impact on the mission of  
2 the Central Intelligence Agency.

3 **“§ 3554. Agency responsibilities”**

4 “(a) IN GENERAL.—The head of each agency shall—

5 “(1) be responsible for—

6 “(A) providing information security protec-  
7 tions commensurate with the risk and mag-  
8 nitude of the harm resulting from unauthorized  
9 access, use, disclosure, disruption, modification,  
10 or destruction of—

11 “(i) information collected or main-  
12 tained by or on behalf of the agency; and

13 “(ii) information systems used or op-  
14 erated by an agency or by a contractor of  
15 an agency or other organization on behalf  
16 of an agency;

17 “(B) complying with the requirements of  
18 this subchapter and related policies, procedures,  
19 standards, and guidelines, including—

20 “(i) information security standards  
21 and guidelines promulgated under section  
22 11331 of title 40 and section 20 of the Na-  
23 tional Institute of Standards and Tech-  
24 nology Act (15 U.S.C. 278g–3);

1                 “(ii) information security standards  
2                 and guidelines for national security sys-  
3                 tems issued in accordance with law and as  
4                 directed by the President; and

5                 “(iii) ensuring the standards imple-  
6                 mented for information systems and na-  
7                 tional security systems of the agency are  
8                 complementary and uniform, to the extent  
9                 practicable;

10                “(C) ensuring that information security  
11                management processes are integrated with  
12                agency strategic and operational planning and  
13                budget processes, including policies, procedures,  
14                and practices described in subsection (c)(2);

15                “(D) as appropriate, maintaining secure  
16                facilities that have the capability of accessing,  
17                sending, receiving, and storing classified infor-  
18                mation;

19                “(E) maintaining a sufficient number of  
20                personnel with security clearances, at the ap-  
21                propriate levels, to access, send, receive and  
22                analyze classified information to carry out the  
23                responsibilities of this subchapter; and

24                “(F) ensuring that information security  
25                performance indicators and measures are in-

1           cluded in the annual performance evaluations of  
2           all managers, senior managers, senior executive  
3           service personnel, and political appointees;

4           “(2) ensure that senior agency officials provide  
5           information security for the information and infor-  
6           mation systems that support the operations and as-  
7           sets under their control, including through—

8                 “(A) assessing the risk and magnitude of  
9                 the harm that could result from the unauthor-  
10                ized access, use, disclosure, disruption, modi-  
11                fication, or destruction of such information or  
12                information system;

13                “(B) determining the levels of information  
14                security appropriate to protect such information  
15                and information systems in accordance with  
16                policies, principles, standards, and guidelines  
17                promulgated under section 11331 of title 40  
18                and section 20 of the National Institute of  
19                Standards and Technology Act (15 U.S.C.  
20                278g–3) for information security classifications  
21                and related requirements;

22                “(C) implementing policies and procedures  
23                to cost effectively reduce risks to an acceptable  
24                level;

1                 “(D) with a frequency sufficient to support  
2                 risk-based security decisions, testing and evalu-  
3                 ating information security controls and tech-  
4                 niques to ensure that such controls and tech-  
5                 niques are effectively implemented and oper-  
6                 ated; and

7                 “(E) with a frequency sufficient to support  
8                 risk-based security decisions, conducting threat  
9                 assessments by monitoring information systems,  
10                 identifying potential system vulnerabilities, and  
11                 reporting security incidents in accordance with  
12                 paragraph (3)(A)(v);

13                 “(3) delegate to the Chief Information Officer  
14                 or equivalent (or a senior agency official who reports  
15                 to the Chief Information Officer or equivalent), who  
16                 is designated as the ‘Chief Information Security Of-  
17                 ficer’, the authority and primary responsibility to de-  
18                 velop, implement, and oversee an agencywide infor-  
19                 mation security program to ensure and enforce com-  
20                 pliance with the requirements imposed on the agency  
21                 under this subchapter, including—

22                 “(A) overseeing the establishment and  
23                 maintenance of a security operations capability  
24                 that through automated and continuous moni-  
25                 toring, when possible, can—

1                 “(i) detect, report, respond to, contain, and mitigate incidents that impair information security and agency information systems, in accordance with policy provided by the Director;

6                 “(ii) commensurate with the risk to information security, monitor and mitigate the vulnerabilities of every information system within the agency;

10                 “(iii) continually evaluate risks posed to information collected or maintained by or on behalf of the agency and information systems and hold senior agency officials accountable for ensuring information security;

16                 “(iv) collaborate with the Director and appropriate public and private sector security operations centers to detect, report, respond to, contain, and mitigate incidents that impact the security of information and information systems that extend beyond the control of the agency; and

23                 “(v) report any incident described under clauses (i) and (ii) to the Federal information security incident center, to other

1           appropriate security operations centers,  
2           and to the Inspector General of the agency,  
3           to the extent practicable, within 24  
4           hours after discovery of the incident, but  
5           no later than 48 hours after such dis-  
6           covery;

7           “(B) developing, maintaining, and over-  
8           seeing an agencywide information security pro-  
9           gram as required by subsection (b);

10          “(C) developing, maintaining, and over-  
11          seeing information security policies, procedures,  
12          and control techniques to address all applicable  
13          requirements, including those issued under sec-  
14          tion 11331 of title 40;

15          “(D) training and overseeing personnel  
16          with significant responsibilities for information  
17          security with respect to such responsibilities;  
18          and

19          “(E) assisting senior agency officials con-  
20          cerning their responsibilities under paragraph  
21          (2);

22          “(4) ensure that the agency has a sufficient  
23          number of trained and cleared personnel to assist  
24          the agency in complying with the requirements of

1       this subchapter, other applicable laws, and related  
2       policies, procedures, standards, and guidelines;

3               “(5) ensure that the Chief Information Security  
4       Officer, in consultation with other senior agency offi-  
5       cials, reports periodically, but not less than annually,  
6       to the agency head on—

7               “(A) the effectiveness of the agency infor-  
8       mation security program;

9               “(B) information derived from automated  
10       and continuous monitoring, when possible, and  
11       threat assessments; and

12               “(C) the progress of remedial actions;

13               “(6) ensure that the Chief Information Security  
14       Officer possesses the necessary qualifications, includ-  
15       ing education, training, experience, and the security  
16       clearance required to administer the functions de-  
17       scribed under this subchapter; and has information  
18       security duties as the primary duty of that official;  
19       and

20               “(7) ensure that components of that agency es-  
21       tablish and maintain an automated reporting mecha-  
22       nism that allows the Chief Information Security Of-  
23       ficer with responsibility for the entire agency, and all  
24       components thereof, to implement, monitor, and hold  
25       senior agency officers accountable for the implemen-

1 tation of appropriate security policies, procedures,  
2 and controls of agency components.

3 “(b) AGENCY PROGRAM.—Each agency shall develop,  
4 document, and implement an agencywide information se-  
5 curity program, approved by the Director and consistent  
6 with components across and within agencies, to provide  
7 information security for the information and information  
8 systems that support the operations and assets of the  
9 agency, including those provided or managed by another  
10 agency, contractor, or other source, that includes—

11 “(1) automated and continuous monitoring,  
12 when possible, of the risk and magnitude of the  
13 harm that could result from the disruption or unau-  
14 thorized access, use, disclosure, modification, or de-  
15 struction of information and information systems  
16 that support the operations and assets of the agen-  
17 cy;

18 “(2) consistent with guidance developed under  
19 section 11331 of title 40, vulnerability assessments  
20 and penetration tests commensurate with the risk  
21 posed to agency information systems;

22 “(3) policies and procedures that—

23 “(A) cost effectively reduce information se-  
24 curity risks to an acceptable level;

25 “(B) ensure compliance with—

1                 “(i) the requirements of this sub-  
2 chapter;

3                 “(ii) policies and procedures as may  
4 be prescribed by the Director, and infor-  
5 mation security standards promulgated  
6 pursuant to section 11331 of title 40;

7                 “(iii) minimally acceptable system  
8 configuration requirements, as determined  
9 by the Director; and

10                 “(iv) any other applicable require-  
11                 ments, including—

12                 “(I) standards and guidelines for  
13                 national security systems issued in ac-  
14                 cordance with law and as directed by  
15                 the President; and

16                 “(II) the National Institute of  
17                 Standards and Technology standards  
18                 and guidance;

19                 “(C) develop, maintain, and oversee infor-  
20                 mation security policies, procedures, and control  
21                 techniques to address all applicable require-  
22                 ments, including those promulgated pursuant  
23                 section 11331 of title 40; and

24                 “(D) ensure the oversight and training of  
25                 personnel with significant responsibilities for in-

1           formation security with respect to such respon-  
2           sibilities;

3           “(4) with a frequency sufficient to support risk-  
4           based security decisions, automated and continuous  
5           monitoring, when possible, for testing and evaluation  
6           of the effectiveness and compliance of information  
7           security policies, procedures, and practices, includ-  
8           ing—

9                 “(A) controls of every information system  
10          identified in the inventory required under sec-  
11          tion 3505(c); and

12                 “(B) controls relied on for an evaluation  
13          under this section;

14                 “(5) a process for planning, implementing, eval-  
15          uating, and documenting remedial action to address  
16          any deficiencies in the information security policies,  
17          procedures, and practices of the agency;

18                 “(6) with a frequency sufficient to support risk-  
19          based security decisions, automated and continuous  
20          monitoring, when possible, for detecting, reporting,  
21          and responding to security incidents, consistent with  
22          standards and guidelines issued by the National In-  
23          stitute of Standards and Technology, including—

24                 “(A) mitigating risks associated with such  
25          incidents before substantial damage is done;

1               “(B) notifying and consulting with the  
2               Federal information security incident center  
3               and other appropriate security operations re-  
4               sponse centers; and

5               “(C) notifying and consulting with, as ap-  
6               propriate—

7                       “(i) law enforcement agencies and rel-  
8               evant Offices of Inspectors General; and

9                       “(ii) any other agency, office, or enti-  
10               ty, in accordance with law or as directed  
11               by the President; and

12               “(7) plans and procedures to ensure continuity  
13               of operations for information systems that support  
14               the operations and assets of the agency.

15               “(c) AGENCY REPORTING.—Each agency shall—

16                       “(1) submit an annual report on the adequacy  
17               and effectiveness of information security policies,  
18               procedures, and practices, and compliance with the  
19               requirements of this subchapter, including compli-  
20               ance with each requirement of subsection (b) to—

21                       “(A) the Director;

22                       “(B) the Committee on Homeland Security  
23               and Governmental Affairs of the Senate;

1                 “(C) the Committee on Oversight and Gov-  
2                 ernment Reform of the House of Representa-  
3                 tives;

4                 “(D) other appropriate authorization and  
5                 appropriations committees of Congress; and

6                 “(E) the Comptroller General;

7                 “(2) address the adequacy and effectiveness of  
8                 information security policies, procedures, and prac-  
9                 tices in plans and reports relating to—

10                 “(A) annual agency budgets;

11                 “(B) information resources management of  
12                 this subchapter;

13                 “(C) information technology management  
14                 under this chapter;

15                 “(D) program performance under sections  
16                 1105 and 1115 through 1119 of title 31, and  
17                 sections 2801 and 2805 of title 39;

18                 “(E) financial management under chapter  
19                 9 of title 31, and the Chief Financial Officers  
20                 Act of 1990 (31 U.S.C. 501 note; Public Law  
21                 101–576);

22                 “(F) financial management systems under  
23                 the Federal Financial Management Improve-  
24                 ment Act of 1996 (31 U.S.C. 3512 note); and

1                 “(G) internal accounting and administrative  
2                 controls under section 3512 of title 31; and  
3                 “(3) report any significant deficiency in a policy,  
4                 procedure, or practice identified under paragraph (1) or (2)—  
5                         “(A) as a material weakness in reporting  
6                 under section 3512 of title 31; and  
7                         “(B) if relating to financial management systems, as an instance of a lack of substantial  
8                 compliance under the Federal Financial Management Improvement Act of 1996 (31 U.S.C.  
9                 3512 note).

13     **“§ 3555. Federal information security incident center**

14     “(a) IN GENERAL.—The Director shall ensure the  
15     operation of a central Federal information security incident center to—

17         “(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

21         “(2) compile and analyze information about incidents that threaten information security;

23         “(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities; and

1               “(4) consult with the National Institute of  
2               Standards and Technology, agencies or offices oper-  
3               ating or exercising control of national security sys-  
4               tems (including the National Security Agency), and  
5               such other agencies or offices in accordance with law  
6               and as directed by the President regarding informa-  
7               tion security incidents and related matters.

8               “(b) NATIONAL SECURITY SYSTEMS.—Each agency  
9 operating or exercising control of a national security sys-  
10 tem shall share information about information security in-  
11 cidents, threats, and vulnerabilities with the Federal infor-  
12 mation security incident center to the extent consistent  
13 with standards and guidelines for national security sys-  
14 tems, issued in accordance with law and as directed by  
15 the President.

16               “(c) REVIEW AND APPROVAL.—The Director shall  
17 review and approve the policies, procedures, and guidance  
18 established in this subchapter to ensure that the incident  
19 center has the capability to effectively and efficiently de-  
20 tect, correlate, respond to, contain, mitigate, and reme-  
21 diate incidents that impair the adequate security of the  
22 information systems of more than one agency. To the ex-  
23 tent practicable, the capability shall be continuous and  
24 technically automated.

1     **“§ 3556. National security systems**

2         “The head of each agency operating or exercising  
3 control of a national security system shall be responsible  
4 for ensuring that the agency—

5             “(1) provides information security protections  
6 commensurate with the risk and magnitude of the  
7 harm resulting from the unauthorized access, use,  
8 disclosure, disruption, modification, or destruction of  
9 the information contained in such system;

10          “(2) implements information security policies  
11 and practices as required by standards and guide-  
12 lines for national security systems, issued in accord-  
13 ance with law and as directed by the President; and  
14          “(3) complies with the requirements of this sub-  
15 chapter.”.

16     **SEC. 3. TECHNICAL AND CONFORMING AMENDMENTS.**

17         (a) TABLE OF SECTIONS IN TITLE 44.—The table  
18 of sections for chapter 35 of title 44, United States Code,  
19 is amended by striking the matter relating to subchapters  
20 II and III and inserting the following:

“SUBCHAPTER II—INFORMATION SECURITY

“See.

“3551. Purposes.

“3552. Definitions.

“3553. Authority and functions of the Director.

“3554. Agency responsibilities.

“3555. Federal information security incident center.

“3556. National security systems.”.

21         (b) OTHER REFERENCES.—

1                   (1) Section 1001(c)(1)(A) of the Homeland Se-  
2         curity Act of 2002 (6 U.S.C. 511(c)(1)(A)) is  
3         amended by striking “section 3532(3)” and inserting  
4         “section 3552(b)”.

5                   (2) Section 2222(j)(5) of title 10, United States  
6         Code, is amended by striking “section 3542(b)(2)”  
7         and inserting “section 3552(b)”.

8                   (3) Section 2223(c)(3) of title 10, United  
9         States Code, is amended, by striking “section  
10      3542(b)(2)” and inserting “section 3552(b)”.

11                  (4) Section 2315 of title 10, United States  
12         Code, is amended by striking “section 3542(b)(2)”  
13         and inserting “section 3552(b)”.

14                  (5) Section 20 of the National Institute of  
15         Standards and Technology Act (15 U.S.C. 278g-3)  
16         is amended—

17                   (A) in subsections (a)(2) and (e)(5), by  
18         striking “section 3532(b)(2)” and inserting  
19         “section 3552(b)”; and

20                   (B) in subsection (e)—

21                   (i) in paragraph (2), by striking “sec-  
22         tion 3532(1)” and inserting “section  
23         3552(b)”; and

## **8 SEC. 4. NO ADDITIONAL FUNDS AUTHORIZED.**

9        No additional funds are authorized to carry out the  
10 requirements of section 3554 of title 44, United States  
11 Code, as amended by section 2 of this Act. Such require-  
12 ments shall be carried out using amounts otherwise au-  
13 thorized or appropriated.

## 14 SEC. 5. EFFECTIVE DATE.

15 This Act (including the amendments made by this  
16 Act) shall take effect 30 days after the date of the enact-  
17 ment of this Act.

